Please sign in at the computer stations

Personnel and Readiness Information Management

Information Assurance & Privacy 2010 Annual Briefing

Personnel and Readiness Information Management

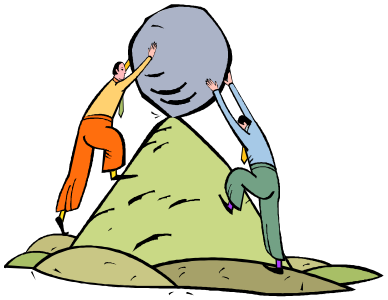
Topics

- Information Assurance (IA)
- Privacy
- Hacking tools and techniques
- Social Media

Information Assurance

Three Basic Facts

- Our jobs rely on accurate, accessible information
- Need to identify information correctly and safeguard appropriately
- Need to balance the accessibility of information with the need to adequately safeguard information



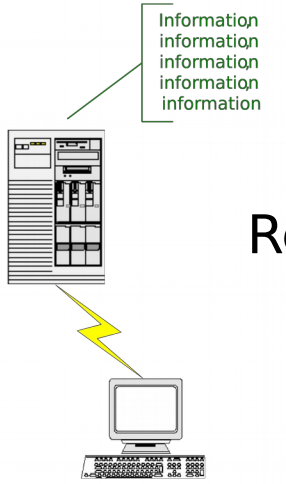
What is IA?

- Measures that protect and defend information and information systems
- IA is really just a collection of methods to provide a risk management approach

Risk Management

- Risk management means
  - Identifying assets
  - Identifying threats and vulnerabilities
  - Identifying impact
  - Providing risk mitigation

Identifying Assets



Information that

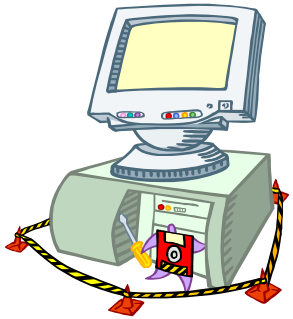
Resides in a **system** that

Connects to an **infrastructure** of some sort

Each level or layer has different protection or mitigation requirements

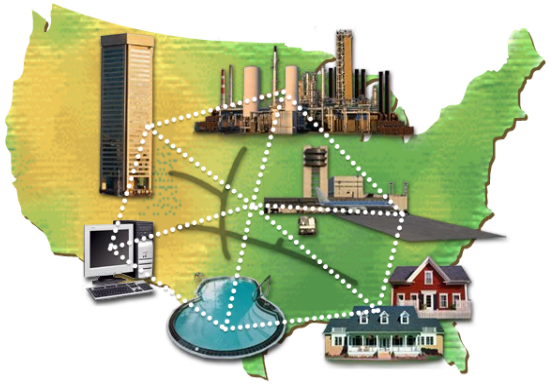
Vulnerabilities and Threats

- Vulnerability
  - Weakness in an information system, cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited
- Threat
  - Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service



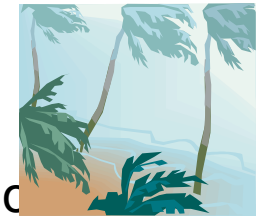
IA Vulnerabilities

- Information
  - No classification or control statements
- System
  - Hardware – no firewalls or sensors
  - Software – glitches or holes in the software
- Infrastructure
  - Increased connectivity creates new vulnerabilities
    - Cascading effects
- Human Factor
- Procedural



Threats to IA

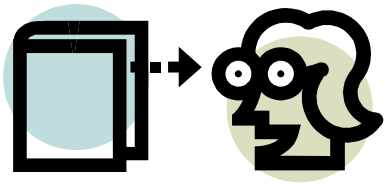
- Threat Categories
  - Natural Threat
    - Natural Events – Fire, hurricane, floo



    - System Environment – Faulty wiring, insufficient HVAC
  - Human Threat
    - Internal – Disgruntled employees
    - External – Spies, hackers

Information Protection

- Information protection such as security classification, Privacy Act, etc.
- Data accuracy, quality, and currency
- Authoritative source
- User training
- User authentication
- Roles and permissions
- Need-to-know



System Protection

- Password protected
- Biometrics
- Email policy
- Regular back-ups
- Software Information Assurance Vulnerability Alerts (IAVAs)
- Virus Protection
- Firewalls

Infrastructure Protection

- Encryption
- Network Design
- Network Firewalls
- DMZs
- Access Control Lists
- Redundancy
- Physical Controls

Worst Mistakes End-Users Make

- Failing to install or keep anti-virus software up-to-date; failing to apply anti-virus to all files
- Opening unsolicited email attachments without verifying source and content
- Executing games, screen savers, or programs from untrusted sources
- Failing to install patches, especially for Microsoft
- Not making and checking backups
- Not installing the security features of your computer and/or network
- Leaving default passwords on your systems

Privacy

DoD Privacy Program Basic Policy

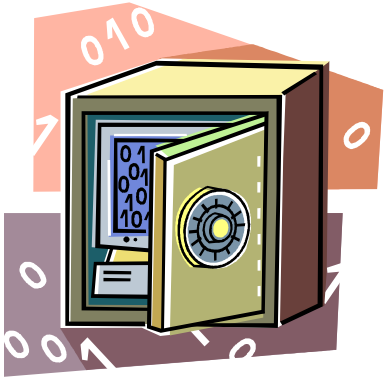
- Privacy Act of 1974 (amended 1988)
  - To regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies
- Section 208 of the E-Government Act of 2002
  - Requires all agencies to conduct PIAs
- Deputy Secretary of Defense Memorandum of June 15, 2005
  - Notifying Individuals When Personal Information is Lost, Stolen, or Compromised (Breach)
- Office of Management and Budget (OMB) Memorandums
  - M-06-15, “Safeguarding Personally Identifiable Information” (May 22, 2006)
  - M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifying Information” (May 22, 2007)
- Social Security Number (SSN) Reduction
  - Dr. Chu Directive – Type Memorandum of March 28, 2008
  - Establishes policy for use of SSN and guidance for reducing its unnecessary use
- Office of the Secretary of Defense for Administration and Management [OSD (A&M)] Memorandum of June 5, 2009
  - Promulgation of current policy

Privacy Act Purpose

- To provide a comprehensive framework regulating how and when the DoD collects, maintains, uses, or disseminates personal information on individuals
- To balance the information requirements and needs of the DoD against the privacy interests and concerns of individuals

We Accomplish This By

- Controlling the Systems of Records that maintain Personally Identifiable Information (PII)
- Controlling access to these systems by authorized persons only
- Controlling the movement and transmission of the PII in those systems
- Managing the human factor through training and awareness



Why You Need to Know About Privacy

- We are collecting, maintaining, distributing, and disposing of information about individuals – Y[illegible]!

- The law requires you to take precautions when collecting, maintaining, distributing, and disposing of PII

Your Responsibilities

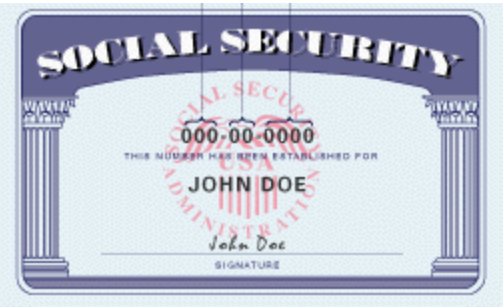
- **Do NOT** maintain records longer than permitted
  - Record retention and destruction are governed by Federal Law and standards
- **Do NOT** destroy records before disposal requirements are met
  - Do use approved shredders or burn bags when disposing of PII
- **Do NOT** transmit PII without ensuring that it is properly marked
  - Do encrypt e-mail
- **Do NOT** use interoffice envelopes to mail PII
- **Do NOT** place PII on shared drives, multi-access calendars, the Intra or Internet that can be accessed by individuals who do not have an official need-to-know
- **Do NOT** leave PII unattended on your desk
  - Do store PII in a desk drawer or locked container

SSN Reduction

DoD Guidance lists 12 cases for Acceptable Uses of SSNs

(Collection, Use, or Retention in any form)

- **Geneva Conventions Serial Number (on a timeline to change/eliminate SSNs from ID cards)**
- **Law Enforcement, National Security, and Credentialing**
- **Security Clearance Investigation or Verification**
- **Interactions with Financial Institutions**
- **Confirmation of Employment Eligibility**
- **Administration of Federal Worker's Compensation**
- **Federal Taxpayer Identification Number**
- **Computer Matching**
- **Foreign Travel**
- **Noncombatant Evacuation Operations**
- **Legacy System Interface**
- **Other Cases (with specified documentation)**



Source: DMDC SSN Reduction Plan Brief, January 25, 2008

SORNs

- Privacy Act System of Records Notices (SORNs)
  - A System of Records is a group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular that is unique to the individual

PIAs

- PIA may or may not relate to a SORN
  - Doesn't need SORN if there is no retrieval by PII
  - PIA set up to cover the gap left by the SORN
- Section 208 of the E-Government Act of 2002 requires all agencies to conduct PIAs for all new or substantially changed information systems that collect, maintain, or disseminate PII on the public
- DoD Instruction 5400.16, DoD PIA Guidance, expands the coverage to include Federal personnel, contractors, and foreign nationals employed at U.S. military facilities internationally
- Structures privacy risk identification and assessment with new DoD PIA Form (DD 2930)

Hacking Tools and Techniques

Keystroke Logging Video

Movie found locally at http://longspur/IATraining2010
Source: CBS News Report retrieved from YouTube

Social Engineering

- Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information
- It is the act of tricking another person into providing information by posing as an individual or agency that is authorized to receive that information or authorized to perform some task
- Techniques may be human or electronic

Phishing

- Phishing
  - Via email or personal interaction
  - Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software
  - A hacker may attempt to gain system information from an employee by posing as a service technician or system administrator with an urgent access problem
- Spear Phishing is a highly targeted phishing attempt
  - The attacker selectively chooses the recipient (target) and usually has a thorough understanding of the target's command or organization
  - The email may appear very genuine
    - Address the recipient by name
    - Use lingo/jargon of the organization
    - Reference actual procedures or DoD Instructions

Pharming

- Pharming
  - A hacker's attack aiming to redirect a website's traffic to another, bogus website
  - Pharming can be conducted either by changing the host's file on a victim's computer or by exploitation of Domain Name Service (DNS) server software
    - DNS servers are computers responsible for resolving Internet domain names into their real addresses
  - Both pharming and phishing have been used for online identity theft information

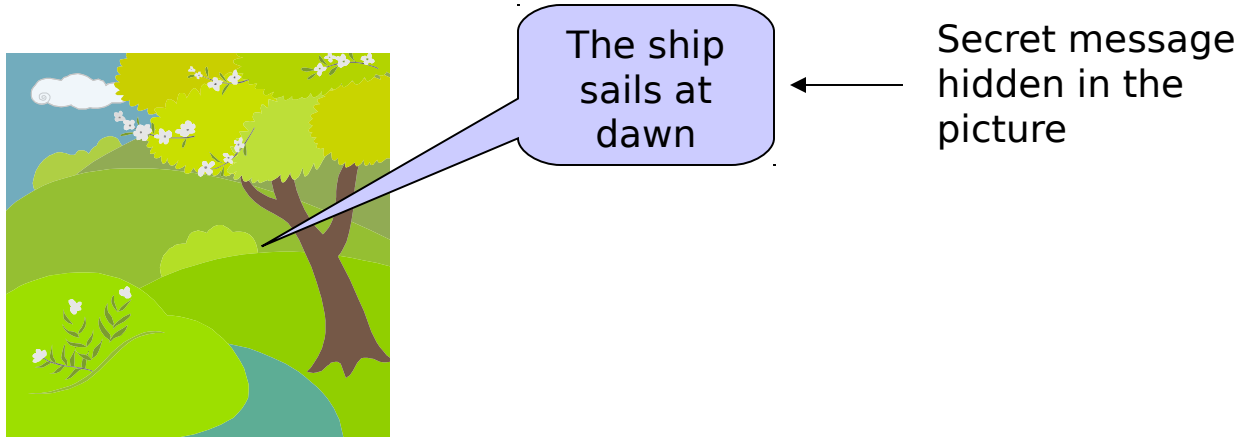
Source: Wikipedia

Not So High Tech

- Dumpster Diving
  - As the name implies
  - Someone goes through the dumpster or trash looking for personal information
    - Credit card receipts, check stubs, billing information

Steganography

- A method of hiding data in another media type so that the existence of the data is concealed
  - In an audio file, graphic, or unused space on a hard drive
  - Usually messages are placed in graphic images by replacing picture bits with message bits
- Steganography tools available as freeware



More on Steganography

- Legitimate uses
  - Watermarking e.g., for copyright purposes
  - Tagging notes to on-line images
- Illegitimate uses
  - Someone stealing data can conceal it in another file or picture
  - It is possible that someone could hide pornography in another file or picture
    - Steganography was the method used by the recently arrested "alleged Russian agents"
  - Messages passed by hiding text in a publicly available web site

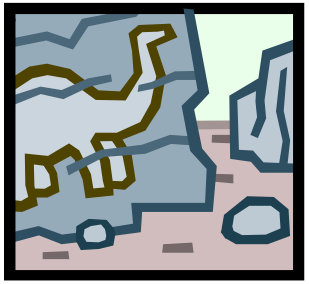


Figure Great Wall of China Steganoperus drawing – precursor to Steganography

Source: Washington Post article, July 1, 2010, Hidden in plain sight

Ways to Protect Yourself

- When in doubt, check it out
- If you receive an email or offer that seems too good to be true, it probably is
  - Foreign dignitary offering you millions to temporarily hold in your bank account, if you send account information
- Don’t know the sender? Don’t open it until you check via another method (e.g., phone) or delete it
- Email from your bank asking for account verification? Not likely. Reputable businesses will not ask you for personal information in an email

Social Media/Social Networking Sites

Social Media and Security Video

Movie found locally at http://longspur/IATraining2010
Source: CNN News Report retrieved from YouTube

Social Media

- Web-based services
- Communities of people who share common interests
- Web interfaces that encompass one or more means of communication
- A shift in how people discover, read, and share news, information and content; transforming monologues (one-to-many) into dialogues (many-to-many)

Why is Social Media so Popular?

- Virtually anyone can join
- Accounts can be created quickly (5 min or less)
- Most are free and don’t bind user to contract
- Convenient interface for users to add or update content on their profile
- Users can share as much or as little as desired
- Easy to connect with friends and family
- “Privacy settings” available on most sit

DoD OKs Social Networking

- Following a ban on social networking by some sectors of the U.S. Department of Defense, the agency has now decided that social networking is integral to its operations and is to be encouraged.

- Last year, for instance, the Marines banned the use of social-networking sites like Facebook, MySpace, and Twitter from its network. With the new policy, the Marines may have to reverse that ban. "Under this new policy, there will be open and consistent access across the board."

- Some agencies, however, have been using sites like Twitter in an official capacity to communicate with the public. In fact, the main Web site for the DoD includes links to Facebook, Twitter, Flickr and YouTube pages.

Source: http://www.pcworld.com/article/190457/us_defense_department_oks_social_networking.html

Social Media: Security Concerns

- Can share as much or as little as desired
- Freedom to post sensitive info about employer, or inappropriate personal info (PII)
- Difficult to distinguish authentic accounts from fraudulent accounts
- Some require only a pre-existing email address to create an account profile
- May be susceptible to known website and browser vulnerabilities (XSS, CSRF, code injection)
- Third-party applications not always approved or sponsored by host social networking site
- Savvy attackers may also aggregate information from multiple sites to gain access to private information (e.g., online banking records, email). For example, you may post your pet's name or birthday on Facebook. That can be used to answer security questions to get access to your banking accounts.

Source: www.nsa.gov/snac

Social Media: Security Concerns

- Impersonation of a friend or colleague can be used to trick users into providing private information or downloading malicious third party applications
- Users can share a variety of multimedia content, from images to video clips to documents. This content has the potential to contain malicious code, which under the right circumstances may cause the user's browser to download malware or perform unintended actions
- Much information might be available through a professional profile such as LinkedIn
- Participation in online discussion groups or blogs might help foreign intelligence services single out disgruntled military or intelligence agency employees who could be recruited or blackmailed

Source: www.nsa.gov/snac

Social Media: a Related Concern

- Social Networking Sites' Data Use Policies
  - "What they know about you and who they share it wit
  - Privacy policies
  - Dossiers of on-line activities
  - Your account information is stored on servers in the internet "cloud" so the company owns that information, not you
    - Can be retrieved by a subpoena
- Most successful internet companies have been those that collect information about users and use that information to sell things
- For every User ID, Facebook keeps a log of the IP address that accessed the account, the data and time, and what exactly the user did – clicking on an ad, looking at someone else's profile, posting a photo, sending a message, etc.

Source: Washington Post, Where web sites see all – and tell all, too, May 29, 2010

Some Social Media Protections

- Consider restricting access to your profile
  - Don’t allow strangers to learn everything they can about you
- Keep your private information private
  - Never post your full name, SSN, address, phone number, financial information, or schedule
  - These will make you vulnerable to identity thieves, scams, burglars, or worse
- Choose a screen name that is different from your real name
  - Avoid using any personal information that would help someone identify or locate you offline
- Think twice before posting your photo
  - Photos can be used to identify you offline
  - They can also be altered or shared without your knowledge
- Don’t post information that makes you vulnerable to a physical attack
  - Revealing where you plan to meet your friends, your schedule, or your street address is almost an open invitation for someone to find you

Some Social Mitigations – Technical

- Keep your OS and web browser up-to-date with latest patches
- Keep virus scanners up-to-date with latest definitions and patches, and scan often
- Refrain from browsing the Internet from privileged accounts (e.g., Administrator, root)
- Click the Logout/Logoff button instead of closing your browser session (XSS, session hijacking)

- Consider clearing your web cache and cookies after browser sessions (XSS)
- Beware of URL shorteners (malicious links)

bit.ly TinyURL.com Goo.gl

Some Social Mitigations – Behavioral

- Perform a risk assessment before posting info about you or your organization
- Confirm connection requests either verbally or face-to-face
- Be selective of third-party applications to add to profile
- Be suspicious of emails from social networking sites

Social Media Risk Assessment

- **LOW RISK – profile has strong privacy settings**
  - Profile searchable by first/last name
  - Name displayed to users not connected to profile
  - Custom connection lists to grant view privileges and/or mask information for specified users
  - Upload information purely about you; this ensures that the privacy of family/friends/neighbors is not compromised by your postings
- **MODERATE RISK – profile has some privacy settings, but ample information loaded about user**
  - Profile searchable by first/last name
  - Name, photo(s), city/town displayed to users not connected to profile
  - Custom connection lists to grant view privileges and/or mask information for specified users
  - Interests/hobbies displayed on profile, but photos include friends and family (all of whom were notified prior to posting)
- **HIGH RISK – profile has no privacy settings, ample information loaded about user**
  - Profile searchable by first/last name, within the site and on well-known search engines
  - Name, photo(s), address, phone number, email address displayed to users not connected to profile
  - Everyone with a web browser can view all content
  - Interests/hobbies displayed, photos include friends and family, along with photo tagging (linking face & name); posted comments that include meeting information (time/place)

Source: www.nsa.gov/snac

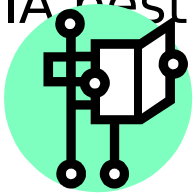
Remember:

- Use your common sense
  - If you are contacted by a stranger on-line, find out if any of your established friends know the person, or run an on-line search on them
  - If something seems too good to be true, it probably is
- Trust your instincts
  - If you feel threatened or uncomfortable during an on-line interaction, don't continue
  - Report any offensive or suspicious behavior to the appropriate persons or agencies
- Be suspicious
  - Don't take any information you receive from a new on-line contact at face value
  - The Internet makes it easy for people to say or do things they would never say or do in public or face-to-face interactions

Protecting yourself is the smart thing to do!

Some Good Sources:

- http://longspur/IATraining2010/IATraining2010.htm
  - IA Training Longspur site containing videos, reference guides, and this presentation
- http://www.onguardonline.gov/topics/overview.aspx
  - General Information regarding network tools and security
  - Geared more towards a family audience
- www.nsa.gov/snac
  - Government specific IA best practices



QUESTIONS?